Technical and organizational measures (TOM)

Contents

This document defines the technical and organizational security measures (TOMs) applied to all standard service offerings provided by Business Network except where a Customer is responsible for security and privacy. Business Network internal organization is aligned to meet specific data protection requirements.

For on premise solutions and otherwise when the security measures depend on customer's security policies or actions taken by customer thereunder, this description applies only if not governed by such customer's policies or actions. Measures described Access Control to premises and facilities shall only apply if the customer uses a Software as a Service (SaaS) solution.

Organization of Information Security

Business Network has a wide-ranging set of information security policies and guidelines based on the ISO/IEC 27000 standard, approved by senior management. The security organization in Business Network includes the Security Manager, Head of Legal affairs, and representatives from all parts of the organization.

Business Network holds the ISO/IEC 27001 certificate, issued in June 2023 that is being renewed and extended in July 2026.

Business Network is committed to corporate security management and development as well as having an objective to ensure undisturbed business operations in all circumstances. The security activities are governed by a commitment to protect employees, information, processes, and assets as well as the corporate reputation.

Site Access Control

For preventing unauthorized persons from gaining access to data processing sites that process or use personal data Business Network has implemented physical access controls. Personal Data stored in professionally hosted data centers with a minimum requirement of an ISO/IEC 27001 certificate. Data processed in qualified premises provide effective physical access control including electronic lock systems, alarm systems and CCTV monitoring.

Access to data centers and premises is granted only to authorized persons. Visitors are always accompanied.

Business Network supports remote and home office work enabling processing of Personal Data outside the secure premises. Business Network ensures Personal Data is processed with adequate security measures outside the office by e.g. for personnel having a security guideline in place required to be followed and awareness of secure remote and home office working in form of reminders and relevant training.

Business Network managed devices are only accepted for work purposes. The devices include technical security controls including anti malware software, intrusion detection and secure transmission capability (e.g. VPN).

System and Data Access Control

Access control ensures systems for Personal Data processing cannot be accessed without authorization and that only authorized persons have access to data so that Personal Data cannot be read, modified, copied, or removed during processing and storage.

Access to Personal Data and systems is granted by following the need-to-know and least privilege principles. All access to systems with Personal Data is granted through a proper process including identification, authentication, and authorization.

Personal user accounts are in use where a user is personally responsible for the account. Special access, including privileged access and shared accounts are granted to an absolute minimum number of users only for a justified need and granted only if a normal user account cannot be used. Privileged access is granted for a limited period. Access is reviewed regularly in systems, and unnecessary access removed.

For common internal systems Single-Sign-On (SSO) is implemented and 2-factor authentication is provided for critical applications and functions.

Transmission Control

To ensure that Personal Data cannot be read, modified, or removed without authorization, personal data is encrypted in transit. Access to internal processing systems are limited by strict access control. Session timeout controls are used for sensitive computer applications and network connections where possible.

Disclosure Control

For preventing accidental or unauthorized disclosure of Personal Data to unauthorized party’s data flows are tracked. All internal data transfers are encrypted and access to systems and data is limited. Internal guidelines exist for employees to prevent accidental or unauthorized disclosure.

Input control

To establish whether and by whom Personal Data has been entered, modified, or removed in data processing systems, only authorized users can access the systems including Personal Data according to access controls. Access to personal data is logged and logs stored preventing unauthorized modification or deletions of events. Access logs are stored for the minimum duration mandated by external compliance requirements.

Order control

For ensuring that Personal Data is processed on behalf of a customer in strict accordance with the customer instructions Business Network provides Data Protection Agreements for signing.

Availability control

For ensuring Personal Data is protected against accidental destruction or loss, Business continuity plans including disaster recovery plans are in place for all services and data is backed up on regular intervals.

Systems and infrastructure for Personal Data storing and processing are designed with resilient service architecture utilizing redundant technologies and minimizing single points of failures. Services are provided including SLAs based on recovery time objectives (RTO) and recovery point objectives (RPO) ensured by service capacity planning and monitoring. Incident Management and Problem Management procedures are in place.

Separation Control

To ensure Personal Data collected for different purposes can be processed separately Business Network stores customers data logically separated based on individual

customer accounts. The data collected for different purposes is also processed separately.

Job control

To ensure Personal Data is processed only in accordance with the Controllers directions Business Network has defined security roles and responsibilities of employees and third parties.

Security responsibilities and tasks are included in the terms and conditions of employment and subcontracting agreements. Relevant commitment to data secrecy or Non-Disclosure Agreements (NDA) are in place with employees and subcontractors, valid after the termination of employment or contract. Personnel screening is carried out to the extent necessary for the role and allowed by effective legislation.

Everyone processing personal data is made aware of security instructions, appropriate handling of assets and information, and required to participate in Security, Personal Data protection and Code of Conduct training provided by Business Network.

Integrity control

Measures designed to ensure that data is authentic and has not been maliciously or accidentally altered during processing, storage or transmission includes checksums and re-transmission for data in transit where needed.

Data retention and deletion control

For ensuring retention and deletion of Personal Data, storage time is defined by the Customer, and Personal Data is deleted in a secure way after expiration of data storage time or immediately when Personal Data is no longer needed. Data on paper (documents, drafts, test materials, production waste, materials defined by Customer for disposal) is physically destroyed locally using secure containers operated by professional disposal companies or a shredder with proper destruction class. Electronic data is deleted using a secure method ensuring no data can be retrieved.

Vulnerability Management

Business Network infrastructure is scanned on a regular basis for vulnerabilities and external penetration tests are performed on all services on a regular basis.

Training and Awareness

Business Network has an extensive training program for all employees, partners and consultants handling personal or corporate data. An onboarding training program for new employees and mandatory yearly training for all employees.

Specific training is also performed for different groups and stakeholders yearly. To ensure Personal Data collected for different purposes can be processed separately Business Network stores customers data logically separated based on individual customer accounts. The data collected for different purposes is also processed separately.

Integrity control

Measures designed to ensure that data is authentic and has not been maliciously or accidentally altered during processing, storage or transmission includes checksums and re-transmission for data in transit where needed.